AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes ~~a cryptographic instruction~~fetch logic, algorithm logic, and execution logic. The fetch logic is disposed within a microprocessor and is configured to receive a cryptographic instruction ~~is received by a computing device~~ as part of an instruction flow executing on ~~the computing device~~said microprocessor. The cryptographic instruction prescribes one of the cryptographic operations and one of a plurality of cryptographic algorithms. The algorithm logic is disposed within said microprocessor and operatively coupled to the cryptographic instruction. The algorithm logic directs the ~~computing device~~microprocessor to execute the one of the cryptographic operations according to the one of a plurality of cryptographic algorithms. The execution logic is disposed within said microprocessor and operatively coupled to the algorithm logic. The execution logic executes the one of the cryptographic operations.

[0022] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a ~~device~~ microprocessor and algorithm logic. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations, where the cryptographic instruction is fetched from memory by fetch logic in the microprocessor. The cryptographic instruction has an algorithm field that prescribes one of a plurality of cryptographic algorithms to be employed when executing the one of the cryptographic operations. The algorithm logic is disposed within the microprocessor and operatively coupled to the cryptography unit. The algorithm logic directs the ~~device~~ microprocessor

to perform the one of the cryptographic operations according to the one of the plurality of cryptographic algorithms.

[0023] Another aspect of the present invention provides a method for performing cryptographic operations in a device. The method includes, within a microprocessor, fetching ~~receiving~~ a cryptographic instruction from memory that prescribes one of a plurality of cryptographic operations and one of a plurality of cryptographic algorithms, and within the microprocessor, executing the one of the cryptographic operations according to the one of the cryptographic algorithms.